

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A)

昭63-293580

⑬ Int.Cl.<sup>4</sup>

識別記号

庁内整理番号

⑭ 公開 昭和63年(1988)11月30日

G 09 C 1/00

7368-5B

G 06 F 12/00

3 0 2

U-8841-5B

12/14

3 2 0

B-7737-5B

審査請求 未請求 発明の数 1 (全10頁)

⑮ 発明の名称 表形式データ暗号化方式

⑯ 特 願 昭62-130786

⑰ 出 願 昭62(1987)5月26日

⑱ 発 明 者 北 澤 具 子 東京都港区芝5丁目33番1号 日本電気株式会社内

⑲ 出 願 人 日本電気株式会社 東京都港区芝5丁目33番1号

⑳ 代 理 人 弁理士 河原 純一

#### 明 細 書

##### 1. 発明の名称

表形式データ暗号化方式

##### 2. 特許請求の範囲

表単位に異なる暗号化のための定義情報を入力する定義情報入力手段と、

この定義情報入力手段により入力された該当する表の暗号の定義情報に基づいて基準コードテーブルのコードのビットを反転するビット反転手段と、

前記定義情報入力手段により入力された該当する表の暗号の定義情報に基づいて基準コードテーブルのコードのビット位置を変換するビット位置変換手段と、

前記ビット反転手段と前記ビット位置変換手段とによって基準コードテーブルから暗号テーブルを作成する暗号テーブル作成手段と、

この暗号テーブル作成手段により作成された暗号テーブルから解読テーブルを作成する解読テーブル作成手段と、

表形式データの暗号化時に暗号化する表形式データを入力するデータ入力手段と、

このデータ入力手段により入力された表形式データを前記暗号テーブル作成手段によって作成された暗号テーブルに従って暗号化するデータ暗号化手段と、

このデータ暗号化手段により暗号化された表形式データを出力する暗号化データ出力手段と、

暗号化された表形式データの解読時に暗号化された表形式データを入力する暗号化データ入力手段と、

この暗号化データ入力手段により入力された暗号化された表形式データを前記解読テーブル作成手段によって作成された解読テーブルに従って解読するデータ解読手段と、

このデータ解読手段により解読された表形式データを出力するデータ出力手段と、

を有することを特徴とする表形式データ暗号化方式。

##### 3. 発明の詳細な説明

## 特開昭63-293580 (2)

## 〔産業上の利用分野〕

本発明は表形式データ暗号化方式に関し、特に表形式データをファイル中の表サブファイルに書き込む際のデータの暗号化および表サブファイルから表形式データを読み込む際のデータの解読を行う表形式データ暗号化方式に関する。

## 〔従来の技術〕

従来、この種の表形式データ暗号化方式としては、プログラム中に固定的に持たれたコード変換表によって表形式データの暗号化を行う方法や、外部記憶装置に固定的に持たれたコード変換表を入力して表形式データの暗号化を行う方法などがあった。

## 〔発明が解決しようとする問題点〕

上述した従来の表形式データ暗号化方式は、固定的に持たれたコード変換表を用いて表形式データの暗号化および解読を行うようになっていたので、コード変換表があれば暗号化された表形式データが容易に解読されてしまう欠点がある。

本発明の目的は、上述の点に鑑み、ファイル中

に表形式データを前記暗号テーブル作成手段によって作成された暗号テーブルに従って暗号化するデータ暗号化手段と、このデータ暗号化手段により暗号化された表形式データを出力する暗号化データ出力手段と、暗号化された表形式データの解読時に暗号化された表形式データを入力する暗号化データ入力手段と、この暗号化データ入力手段により入力された暗号化された表形式データを前記解読テーブル作成手段によって作成された解読テーブルに従って解読するデータ解読手段と、このデータ解読手段により解読された表形式データを出力するデータ出力手段とを有する。

## 〔作用〕

本発明の表形式データ暗号化方式では、定義情報入力手段が表単位に異なる暗号化のための定義情報を入力し、ビット反転手段が定義情報入力手段により入力された該当する表の暗号の定義情報に基づいて基準コードテーブルのコードのビットを反転し、ビット位置変換手段が定義情報入力手段により入力された該当する表の暗号の定義情報

の表サブファイルに書き込まれた表形式データが容易に解読されることがないようにした表形式データ暗号化方式を提供することにある。

## 〔問題点を解決するための手段〕

本発明の表形式データ暗号化方式は、表単位に異なる暗号化のための定義情報を入力する定義情報入力手段と、この定義情報入力手段により入力された該当する表の暗号の定義情報に基づいて基準コードテーブルのコードのビットを反転するビット反転手段と、前記定義情報入力手段により入力された該当する表の暗号の定義情報に基づいて基準コードテーブルのコードのビット位置を変換するビット位置変換手段と、前記ビット反転手段と前記ビット位置変換手段とによって基準コードテーブルから暗号テーブルを作成する暗号テーブル作成手段と、この暗号テーブル作成手段により作成された暗号テーブルから解読テーブルを作成する解読テーブル作成手段と、表形式データの暗号化時に暗号化する表形式データを入力するデータ入力手段と、このデータ入力手段により入力さ

に基づいて基準コードテーブルのコードのビット位置を変換し、暗号テーブル作成手段がビット反転手段とビット位置変換手段とによって基準コードテーブルから暗号テーブルを作成し、解読テーブル作成手段が暗号テーブル作成手段により作成された暗号テーブルから解読テーブルを作成し、データ入力手段が表形式データの暗号化時に暗号化する表形式データを入力し、データ暗号化手段がデータ入力手段により入力された表形式データを暗号テーブル作成手段によって作成された暗号テーブルに従って暗号化し、暗号化データ出力手段がデータ暗号化手段により暗号化された表形式データを出力し、暗号化データ入力手段が暗号化された表形式データの解読時に暗号化された表形式データを入力し、データ解読手段が暗号化データ入力手段により入力された暗号化された表形式データを解読テーブル作成手段によって作成された解読テーブルに従って解読し、データ出力手段がデータ解読手段により解読された表形式データを出力する。

## 特開昭63-293580 (3)

## (実施例)

次に、本発明について図面を参照して詳細に説明する。

第1図は、本発明の表形式データ暗号化方式の一実施例の構成を示すブロック図である。本実施例の表形式データ暗号化方式は、表サブファイル17aを格納するファイル17と、ファイル17中の表サブファイル17aのオープン時に暗号テーブル13と解読テーブル14とを作成する表サブファイルオープン処理部100と、表形式データ15をファイル17中の表サブファイル17aに書き込むときに表形式データ15を暗号テーブル13に基づいて暗号化するデータ暗号化処理部200と、ファイル17中の表サブファイル17aから暗号化された表形式データ18を読み込むときに暗号化された表形式データ18を解読テーブル14に基づいて解読するデータ解読処理部300とから、その主要部が構成されている。

表サブファイルオープン処理部100は、該当する表の暗号化のための定義情報12を入力する定義情報入力手段1と、定義情報入力手段1によって

15を1バイト単位で暗号テーブル13中の対応するコードに置き換えて暗号化するデータ暗号化手段7と、データ暗号化手段7により暗号化された表形式データ16をファイル17中の表サブファイル17aに書き込む暗号化データ出力手段8とを含んで構成されている。

データ解読処理部300は、ファイル17中の表サブファイル17aから暗号化された表形式データ18を入力する暗号化データ入力手段9と、暗号化データ入力手段9によりファイル17中の表サブファイル17aから暗号化された表形式データ18を読み込み解読テーブル作成手段5によって作成された256バイトの解読テーブル14を用いて読み込んだ暗号化された表形式データ18を1バイト単位で解読テーブル14中の対応するコードに置き換えて解読するデータ解読手段10と、解読された表形式データ19を出力するデータ出力手段11とを含んで構成されている。

表形式データ15、16、18および19は可変長データであり、例えば第2図に表形式データ15を例に

入力された該当する表の暗号化のための定義情報12を基に第5図に示す8ビットの組合せの全ケースである256バイトの全コードを昇順に並べたテーブル（以下、基準コードテーブルと称する）の各コードの1バイト中のある位置のビットを反転させるビット反転手段3および基準コードテーブルの各コードの1バイト中のビットの位置を入れるビット位置変換手段2を用いて256バイトの全コードを暗号化したときのコード変換表である暗号テーブル13を作成する暗号テーブル作成手段4と、暗号テーブル作成手段4により作成された暗号テーブル13を基に256バイトの全コードを解読したときのコード変換表である解読テーブル14を作成する解読テーブル作成手段5とを含んで構成されている。

データ暗号化処理部200は、表形式データ15を入力するデータ入力手段6と、データ入力手段6により暗号化する表形式データ15を入力し暗号テーブル作成手段4によって作成された256バイトの暗号テーブル13を用いて入力した表形式データ

として示すように、データの全バイト長15aおよびフィールド数15bからなる制御部15cと、フィールド長15dおよびフィールド長15d分のフィールドデータ15eの繰返しからなるデータ部15fとから構成されている。

第3図を参照すると、定義情報12は、1バイト中の左からのビットの順序に対応してそれぞれ移動先のビットの位置を指定している0から7までの順列であるビット位置変換情報12aと、1バイト中の左からのビットの順序に対応してオン（1）は反転する、オフ（0）は反転しないことを意味するオンおよびオフの8ビットの組合せで反転するビットを指定しているビット反転情報12bとから構成されている。

次に、このように構成された本実施例の表形式データ暗号化方式の動作について説明する。

まず、ファイル17中の表サブファイル17aに対する表形式データの入出力に先立って、表サブファイルオープン処理部100が起動されてファイル17中の表サブファイル17aのオープン処理が行わ

## 特開昭63-293580 (4)

れる。このとき、暗号化に用いる暗号テーブル13と解読に用いる解読テーブル14との作成も同時に行われる。

定義情報入力手段1によって該当する表をどのように暗号化するかを規定する定義情報12が入力される。定義情報12は、表ごとに異なる定義を与えることが可能である。なお、本実施例では、具体的に第4図に示す定義情報12が入力されたものとして説明を行う。

1バイトのデータは、8ビットの組合せとして00000000(2進)から11111111(2進)までの2の8乗、つまり256の組合せがあるが、この256の組合せを昇順に並べると先頭からの変位と、その変位にある1バイトの値とが一致する第5図に示すような基準コードテーブルが得られる。この基準コードテーブルを第4図に示した定義情報12により暗号テーブル13に変換する。つまり、暗号テーブル13は、暗号テーブル13の先頭から何バイト目にあるかという変位が暗号化される前の1バイトのコードの値を示すことに

なる。

まず、第4図に示した定義情報12に基づいてビット位置変換手段2を用いてビット位置の変換を行うが、256バイトを昇順に並べた基準コードテーブル中の、例えばC1(16進)のコードがどのように暗号テーブル13のコードに変換されるかが第9図に示されている。定義情報12では、0ビット目を4ビット目に、1ビット目を5ビット目に、2ビット目を6ビット目に、3ビット目を7ビット目に、4ビット目を0ビット目に、5ビット目を1ビット目に、6ビット目を2ビット目に、7ビット目を3ビット目にそれぞれ置き換える指定なので、ビット位置の変換をビット位置変換手段2を用いて行くと、第9図に示すように、C1(16進)のコードは1C(16進)になる。さらに、この1C(16進)に対してビット反転手段3を用いて定義情報12に指定されているように0ビット目と4ビット目とを反転するとコードは94(16進)となり、これが暗号テーブル13の変位C1(16進)に対応する暗号コードとなる。この変換を

第5図の256バイト全てについて行くと、まずビット位置変換手段2によって第6図に示すテーブルとなり、さらにビット反転手段3によって第7図に示す暗号テーブル13が完成する。

なお、本実施例では、先にビット位置変換手段2によるビット位置変換処理を行い、次にビット反転手段3によるビット反転処理を行ったが、この順序を入れ替えて先にビット反転手段3によるビット反転処理を行い、次にビット位置変換手段2によるビット位置変換処理を行う方法もある。

解読テーブル作成手段5では、暗号化された表形式データ18を解読するための解読テーブル14を作成するが、この解読テーブル14は暗号テーブル13を用いて作成する。暗号テーブル13は、暗号テーブル13の先頭からの変位の値をもつ1バイトのコードをその変位にある1バイトの値と入れ換えて暗号化するので、解読テーブル14は、第10図に示すように、暗号化された1バイトの値の変位にある1バイトのコードを変位とし変位を解読されたコードとしておけば解読できることになる。そ

こで、暗号テーブル13の256バイトについて、暗号テーブル13の先頭からの変位の値を暗号テーブル13のその変位にある1バイトの値と一致する解読テーブル14の変位に1バイトのコードとして入れていけば、第8図に示すような解読テーブル14が作成できる。

次に、表形式データ15の暗号化を行うためにデータ暗号化処理部200が起動されると、まず暗号化する表形式データ15がデータ入力手段6を用いて入力される。入力された表形式データ15は、データ暗号化手段7により暗号テーブル13を用いて暗号化されるが、入力された表形式データ15のデータ部15fのみが暗号化される。表形式データ15の制御部15cについては、暗号化するときおよび解読するときデータ部15fの全バイト長15aが必要であるために暗号化しない。表形式データ15のデータ部15fを1バイトずつにして、暗号テーブル13のその1バイトの値の変位にあるコードに置き換える。

例えば、第11図に示すように、データ部15cが

## 特開昭63-293580 (6)

0 2 C 1 C 2 0 1 C 3 (16進) というデータが入力されたとすると、まず0 2は第7図に示す暗号テーブル13の変位0 2 (16進)にあるコードA 8 (16進)と置き換え、C 1は暗号テーブル13の変位C 1 (16進)にあるコード9 4 (16進)と置き換え、C 2は暗号テーブル13の変位C 2 (16進)にあるコードA 4 (16進)と置き換え、0 1は暗号テーブル13の変位0 1 (16進)にあるコード9 8 (16進)と置き換え、C 3は暗号テーブル13の変位C 3 (16進)にあるコードB 4 (16進)と置き換えることによって、データ部0 2 C 1 C 2 0 1 C 3 (16進)は、A 8 9 4 A 4 9 8 B 4 (16進)と暗号化される。

このようにして暗号化された表形式データ16は、暗号化データ出力手段8によってファイル17中の表サブファイル17aに書き込まれる。本実施例の表形式データ暗号化方式では、可変長の表形式データ15のデータ部15fをフィールド長15dを含めて暗号化することによって、より一層暗号化の効果があがるようになっている。

置き換え、B 4 (16進)は解読テーブル14の変位B 4 (16進)にあるコードC 3 (16進)と置き換えることによって、暗号化された表形式データ18のデータ部A 8 9 4 A 4 9 8 B 4 (16進)は0 2 C 1 C 2 0 1 C 3 (16進)と解読される。

第11図および第12図の例は、表形式データ15のデータ部15fを暗号化しA 8 9 4 A 4 9 8 B 4 (16進)となり、それを解読して元の表形式データ15のデータ部15fと同一の表形式データ18のデータ部0 2 C 1 C 2 0 1 C 3 (16進)を得たことになる。

## (発明の効果)

以上説明したように本発明は、表単位に暗号化のための定義情報を与えて暗号化および解読の際に使用されるコード変換表である暗号テーブルおよび解読テーブルを定義情報から動的に作成することにより、コード変換表を固定的に持つ場合に比べて暗号化された表形式データの解読が格段的に困難になり、機密保護に効果がある。特に、表形式データのデータ部のフィールド長も含めて暗

号化を行えるので、さらに機密保護に効果がある。

続いて、ファイル17中の表サブファイル17aに書き込まれたデータを解読するためにデータ解読処理部300が起動されると、まず暗号化された表形式データ18を暗号化データ入力手段9を用いてファイル17中の表サブファイル17aから読み込む。読み込まれた暗号化された表形式データ18は、データ解読手段10によって解読されるが、暗号化された表形式データ18を1バイトずつにしてそれぞれ解読テーブル14のその1バイトの値の変位にあるコードに置き換える。

例えば、第12図に示すA 8 9 4 A 4 9 8 B 4 (16進)という暗号化された表形式データ18のデータ部を解読すると、まずA 8 (16進)は第8図に示す解読テーブル14の変位A 8 (16進)にあるコード0 2 (16進)と置き換え、9 4 (16進)は解読テーブル14の変位9 4 (16進)にあるコードC 1 (16進)と置き換え、A 4 (16進)は解読テーブル14の変位A 4 (16進)にあるコードC 2 (16進)と置き換え、9 8 (16進)は解読テーブル14の変位9 8 (16進)にあるコード0 1 (16進)と

号化を行えるので、さらに機密保護に効果がある。

## 4. 図面の簡単な説明

第1図は本発明の一実施例の構成を示すブロック図、

第2図は第1図中の表形式データの構成を示す図、

第3図は第1図中の定義情報の構成を示す図、

第4図は第3図に示した定義情報の具体例を示す図、

第5図は256バイトのコードを昇順に並べた基準コードテーブルを示す図、

第6図は第5図に示した基準コードテーブルに対して第1図中のビット位置変換手段によりビット位置変換処理を実行して得られたテーブルを示す図、

第7図は第6図に示したテーブルに第1図中のビット反転手段によりビット反転処理を実行して得られた暗号テーブルを示す図、

第8図は第7図に示した暗号テーブルから第1図中の解読テーブル作成手段により作成された解

## 特開昭63-293580 (6)

読テーブルを示す図、

第9図は第5図に示した基準コードテーブルを第7図に示した暗号テーブルに変換する処理の一例を示す図、

第10図は第7図に示した暗号テーブルから第8図に示した解読テーブルを作成する処理の一例を示す図、

第11図は表形式データを第7図に示した暗号テーブルを用いて暗号化する処理の一例を示す図、

第12図は表形式データを第8図に示した解読テーブルを用いて解読する処理の一例を示す図である。

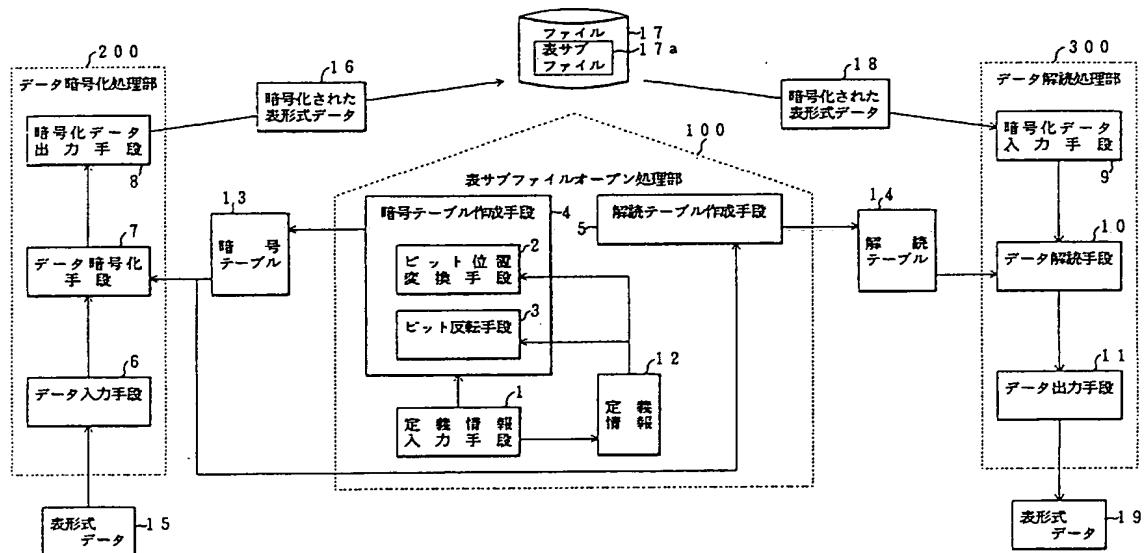
図において、

- 1・・・定義情報入力手段、
- 2・・・ビット位置変換手段、
- 3・・・ビット反転手段、
- 4・・・暗号テーブル作成手段、
- 5・・・解読テーブル作成手段、
- 6・・・データ入力手段、
- 7・・・データ暗号化手段、

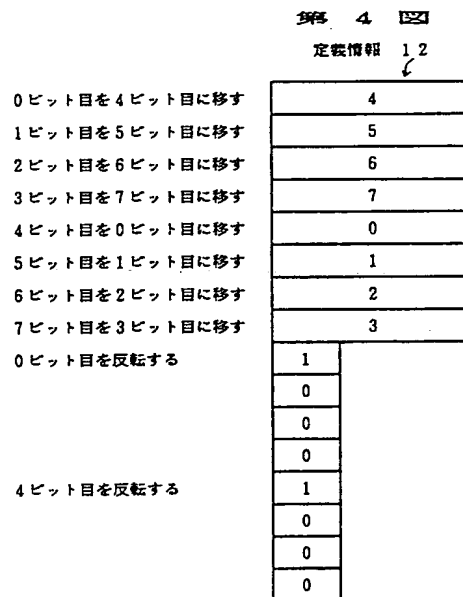
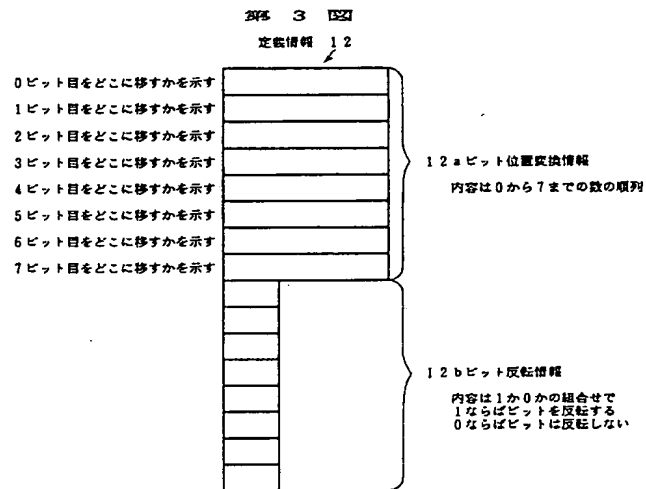
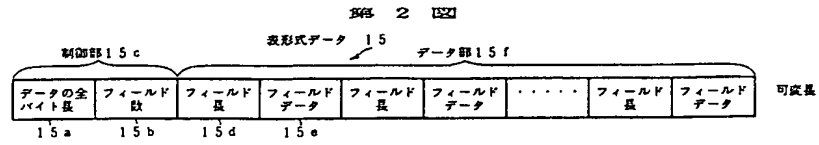
- 8・・・暗号化データ出力手段、
- 9・・・暗号化データ入力手段、
- 10・・・データ解読手段、
- 11・・・データ出力手段、
- 12・・・定義情報、
- 13・・・暗号テーブル、
- 14・・・解読テーブル、
- 15・・・表形式データ、
- 16・・・暗号化された表形式データ、
- 17・・・ファイル、
- 17a・・・表サブファイル、
- 18・・・暗号化された表形式データ、
- 19・・・表形式データである。

特許出願人 日本電気株式会社  
代理人 弁理士 河原 純一

第 1 図



特開昭63-293580 (7)



特開昭63-293580 (8)

## 第 5 図

```

000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBF
C0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF

```

256バイトのコードを昇順に並べた基準コードテーブル(16進にて表示)  
 基準コードテーブルの先頭からの変位とその変位にある1バイトの値とは一致する

## 第 6 図

```

00102030405060708090A0B0C0D0E0F001112131415161718191A1B1C1D1E1F1
02122232425262728292A2B2C2D2E2F203132333435363738393A3B3C3D3E3F3
04142434445464748494A4B4C4D4E4F405152535455565758595A5B5C5D5E5F5
06162636465666768696A6B6C6D6E6F607172737475767778797A7B7C7D7E7F7
08182838485868788898A8B8C8D8E8F809192939495969798999A9B9C9D9E9F9
0A1A2A3A4A5A6A7A8A9AAABACADAFAFA0B1B2B3B4B5B6B7B8B9BABBBCBDBEBFB
0C1C2C3C4C5C6C7C8C9CACBCCCDCECF0D1D2D3D4D5D6D7D8D9DADBDCDDDEDFD
0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFE0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF

```

256バイトのコードを昇順に並べた基準コードテーブル(第5図)にビット位置変換手段2を  
 実行してビット位置を変換して得られたテーブル



特開昭63-293580 (9)

## 第 7 図

```

8898A8B8C8D8E8F808182838485868788999A9B9C9D9E9F90919293949596979
8A9AAABACADAEAF0A1A2A3A4A5A6A7A8B9BABBBBCDBEBFB0B1B2B3B4B5B6B7B
8C9CACBCCCDCECF0C1C2C3C4C5C6C7C8D9DADBDCDDDEDFD0D1D2D3D4D5D6D7D
8E9EAEBECEDEEEFE0E1E2E3E4E5E6E7E8F9FAFBFCFDFEFFFF0F1F2F3F4F5F6F7F
8090A0B0C0D0E0F000102030405060708191A1B1C1D1E1F10111213141516171
8292A2B2C2D2E2F202122232425262728393A3B3C3D3E3F30313233343536373
8494A4B4C4D4E4F404142434445464748595A5B5C5D5E5F50515253545556575
8696A6B6C6D6E6F606162636465666768797A7B7C7D7E7F70717273747576777

```

第6図のビット位置変換手段2を実行して得られたテーブルに対して  
ビット反転手段3を実行して完成した暗号テーブル13

## 第 8 図

```

8898A8B8C8D8E8F808182838485868788999A9B9C9D9E9F90919293949596979
8A9AAABACADAEAF0A1A2A3A4A5A6A7A8B9BABBBBCDBEBFB0B1B2B3B4B5B6B7B
8C9CACBCCCDCECF0C1C2C3C4C5C6C7C8D9DADBDCDDDEDFD0D1D2D3D4D5D6D7D
8E9EAEBECEDEEEFE0E1E2E3E4E5E6E7E8F9FAFBFCFDFEFFFF0F1F2F3F4F5F6F7F
8090A0B0C0D0E0F000102030405060708191A1B1C1D1E1F10111213141516171
8292A2B2C2D2E2F202122232425262728393A3B3C3D3E3F30313233343536373
8494A4B4C4D4E4F404142434445464748595A5B5C5D5E5F50515253545556575
8696A6B6C6D6E6F606162636465666768797A7B7C7D7E7F70717273747576777

```

第7図の暗号テーブル13から作成した解読テーブル14

特開昭63-293580 (10)

図 9

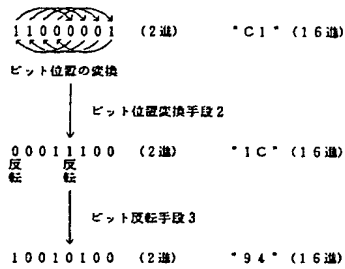


図 10

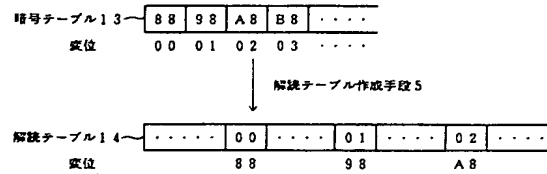


図 11

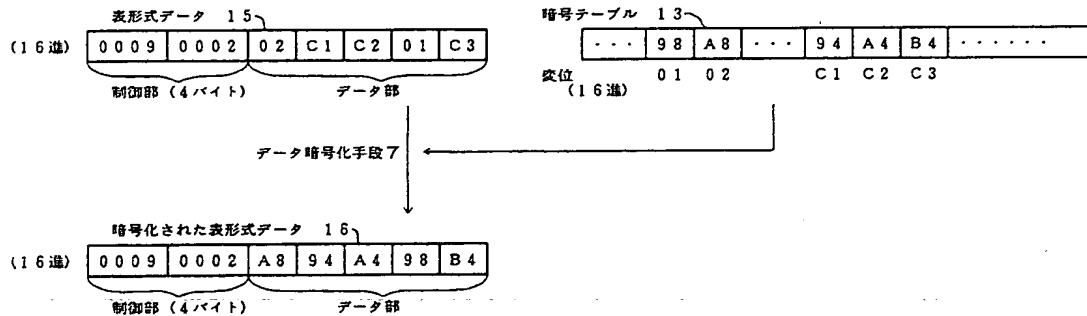


図 12

